(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 09298736 A

(43) Date of publication of application: 18 . 11 . 97

(51) Int. Cl H04N 7/167
G09C 1/00
H04L 9/22
H04L 9/36

(21) Application number: 08113598

(22) Date of filing: 08 . 05 . 96

(71) Applicant: MATSUSHITA ELECTRIC IND CO LTD

(72) Inventor: HATAKEYAMA TAKESHI
MURAKAMI HIRONORI
KATSUTA NOBORU
IBARAKI SUSUMU

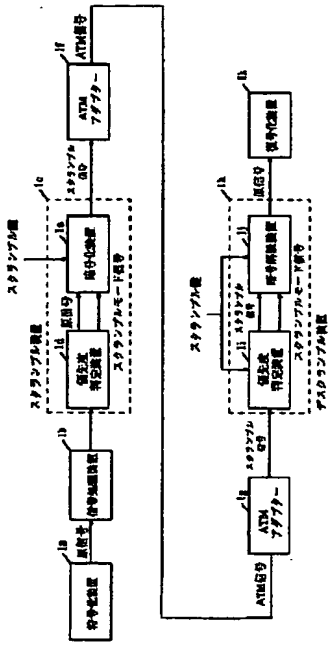
# (54) SCRAMBLE TRANSMITTER, SCRAMBLER, DESCRAMBLER AND SIGNAL PROCESSOR

(57) Abstract:

PROBLEM TO BE SOLVED: To realize effect control and reduction on packet abort in the scramble transmitter to limit a party to reproduce digital coded data with priority.

SOLUTION: A scrambler 1c conducts scrambling by revising the scramble mode depending on priority relating to packet abort to obtain a scramble signal. A descrambler 1h conducts processing reverse to above to obtain a reproduction signal. Through the constitution above, scrambling is applied to packets with low priority to realize effect control or series of ciphers with a chain are divided depending on the priority to reduce the effect on packet abort.





(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

**特開平9－298736**

(43)公開日　平成９年(1997)11月18日

| (51)Int.Cl.[6] | | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|---|
| Ｈ０４Ｎ | 7/167 | | | Ｈ０４Ｎ | 7/167 | Ｚ |
| Ｇ０９Ｃ | 1/00 | ６６０ | 7259－5Ｊ | Ｇ０９Ｃ | 1/00 | ６６０Ｅ |
| Ｈ０４Ｌ | 9/22 | | | Ｈ０４Ｌ | 9/00 | ６５５ |
| | 9/36 | | | | | ６８５ |

審査請求　未請求　請求項の数23　ＯＬ　（全 19 頁）

(21)出願番号　特願平8－113598

(22)出願日　平成８年(1996)５月８日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　畠山　武士
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　村上　弘規
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　勝田　昇
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　岡田　和秀

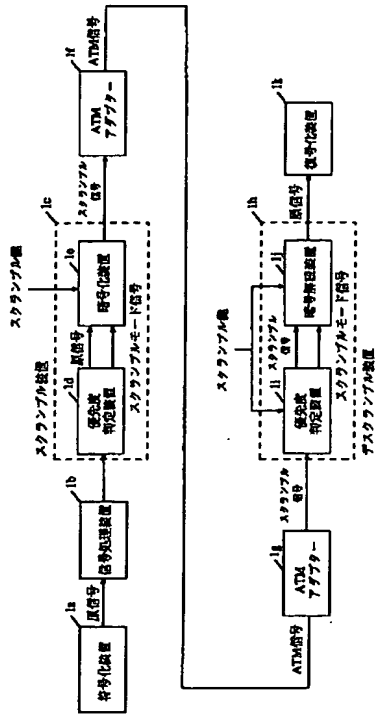
最終頁に続く

(54)【発明の名称】　スクランブル伝送装置およびスクランブル装置およびデスクランブル装置および信号処理装置

(57)【要約】

【課題】　優先度を有するディジタル符号化されたデータの再生に際して、その再生者を限定するためのスクランブル伝送装置に関するもので、効果制御やパケット廃棄への影響の低減を実現するスクランブル伝送装置を提供する。

【解決手段】　スクランブル装置1cは、パケット廃棄に関する優先度に応じてスクランブルモードを変更してスクランブルを行い、スクランブル信号を得る。デスクランブル装置1hでは、逆処理を行い、再生信号を得る。このような構成により、低優先度のパケットにのみスクランブルを行い、効果制御を実現したり、優先度に応じて連鎖のある暗号の系列を分け、パケット廃棄への影響を低減したスクランブル伝送装置を実現する。



1

【特許請求の範囲】

【請求項１】　スクランブル装置とデスクランブル装置とを具備し、前記スクランブル装置は、パケット廃棄に関する優先度に応じて異なるスクランブルモードでスクランブルを行うように構成され、前記デスクランブル装置は、前記スクランブル装置からのデータについて前記パケット廃棄に関する優先度に応じて前記異なるスクランブルモードでデスクランブルを行うように構成されていることを特徴とするスクランブル伝送装置。

【請求項２】　スクランブル装置が優先度判定装置と暗号化装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、前記パケット廃棄に関する優先度を判定し、前記暗号化装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号化装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきスクランブルを行うように構成されていることを特徴とする請求項１に記載のスクランブル伝送装置。

【請求項３】　デスクランブル装置が優先度判定装置と暗号解読装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、前記パケット廃棄に関する優先度を有するパケットの優先度を判定し、前記暗号解読装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号解読装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきデスクランブルを行うように構成されていることを特徴とする請求項１に記載のスクランブル伝送装置。

【請求項４】　スクランブル装置は、パケット廃棄に関する優先度が高優先度のパケットについてはスクランブルを行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはスクランブルを行うように構成されていることを特徴とする請求項１に記載のスクランブル伝送装置。

【請求項５】　デスクランブル装置は、スクランブル鍵を有する場合には、パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはデスクランブルを行い、かつ、前記スクランブル鍵を有しない場合には、前記パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケット廃棄に関する優先度が低優先度のパケットについては廃棄を行うように構成されていることを特徴とする請求項１に記載のスクランブル伝送装置。

【請求項６】　スクランブル装置は、連鎖のある暗号方式でスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてスクランブルを行うように構成されていることを特徴とする請求項１に記載のスクランブル伝送装置。

2

【請求項７】　デスクランブル装置は、連鎖のある暗号方式でデスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてデスクランブルを行うように構成されていることを特徴とする請求項１に記載のスクランブル伝送装置。

【請求項８】　２つの連続するパケットを単位として処理を行い、２つのパケットのうち一方のパケットのパケット廃棄に関する優先度が高優先度のパケットの場合には２つのパケットの両方を高優先度のパケットに書き換えて出力する信号処理装置を付加していることを特徴とする請求項１に記載のスクランブル伝送装置。

【請求項９】　パケット廃棄に関する優先度が、ＭＰＥＧ２トランスポートストリームにおけるトランスポートパケットの優先度を示す１ビットのフラグtransport _priorityであることを特徴とする請求項１に記載のスクランブル伝送装置。

【請求項１０】　パケット廃棄に関する優先度に応じて異なるスクランブルモードでスクランブルを行うように構成されていることを特徴とするスクランブル装置。

【請求項１１】　優先度判定装置と暗号化装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、入力されたパケットの前記パケット廃棄に関する優先度を判定し、前記暗号化装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号化装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきスクランブルを行うように構成されていることを特徴とする請求項１０に記載のスクランブル装置。

【請求項１２】　パケット廃棄に関する優先度が高優先度のパケットについてはスクランブルを行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはスクランブルを行うように構成されていることを特徴とする請求項１０に記載のスクランブル装置。

【請求項１３】　連鎖のある暗号方式でスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてスクランブルを行うように構成されていることを特徴とする請求項１０に記載のスクランブル装置。

【請求項１４】　パケット廃棄に関する優先度が、ＭＰＥＧ２トランスポートストリームにおけるトランスポートパケットの優先度を示す１ビットのフラグtransport _priorityであることを特徴とする請求項１０に記載のスクランブル装置。

【請求項１５】　パケット廃棄に関する優先度に応じて異なるスクランブルモードでデスクランブルを行うように構成されていることを特徴とするデスクランブル装置。

【請求項１６】　優先度判定装置と暗号解読装置とを具

備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、入力されたパケットの前記パケット廃棄に関する優先度を判定し、前記暗号解読装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号解読装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきデスクランブルを行うように構成されていることを特徴とする請求項１５に記載のデスクランブル装置。

【請求項１７】　スクランブル鍵を有する場合には、パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはデスクランブルを行い、かつ、前記スクランブル鍵を有しない場合には、前記パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケットに関する優先度が低優先度のパケットについては廃棄を行うように構成されていることを特徴とする請求項１５に記載のデスクランブル装置。

【請求項１８】　連鎖のある暗号方式でデスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてデスクランブルを行うように構成されていることを特徴とする請求項１５に記載のデスクランブル装置。

【請求項１９】　パケット廃棄に関する優先度が、ＭＰＥＧ２トランスポートストリームにおけるトランスポートパケットの優先度を示す１ビットのフラグtransport_priorityであることを特徴とする請求項１５に記載のデクランブル装置。

【請求項２０】　パケット廃棄に関する優先度を有するパケットを入力とし、入力された２つの連続するパケットを単位として処理を行い、２つのパケットのうち一方のパケットのパケット廃棄に関する優先度が高優先度のパケットの場合には２つのパケットの両方を高優先度のパケットに書き換えてスクランブル装置に出力するように構成されていることを特徴とするスクランブル伝送装置用の信号処理装置。

【請求項２１】　パケット廃棄に関する優先度が、ＭＰＥＧ２トランスポートストリームにおけるトランスポートパケットの優先度を示す１ビットのフラグtransport_priorityであることを特徴とする請求項２０に記載のスクランブル伝送装置用の信号処理装置。

【請求項２２】　２つの連続するパケットを単位として処理を行うことに代えて、３つ以上の連続するパケットを単位として処理を行うように構成してあることを特徴とする請求項８に記載のスクランブル装置。

【請求項２３】　２つの連続するパケットを単位として処理を行うことに代えて、３つ以上の連続するパケットを単位として処理を行うように構成してあることを特徴とする請求項２０のスクランブル伝送装置用の信号処理装置。



【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタル符号化されたデータの伝送に際し、信号をスクランブルし、デスクランブル手順を許可されたものだけに与えることによって、再生できる者を限定するスクランブル伝送装置、およびこのスクランブル伝送装置を構成するスクランブル装置、およびデスクランブル装置、およびパケット廃棄に関する優先度の変換を行う信号処理装置に関するものであって、パケット廃棄に関する優先度を用いることによって、効果制御、パケット廃棄によるエラー伝搬の低減などを実現するスクランブル伝送装置、スクランブル装置、デスクランブル装置、信号処理装置に関するものである。

【０００２】

【従来の技術】従来のディジタル信号に対するスクランブル伝送装置としては、連鎖のあるブロック暗号方式により入力信号を暗号化する方法があった。たとえば、「現代暗号理論」（電子情報通信学会編）第４章に、連鎖のあるブロック暗号方式を用いた暗号化方法に関する記述がある。

【０００３】ブロック暗号方式とは、暗号化するデータを固定長のブロックに分解して、ブロックごとに暗号化する方式であり、連鎖のあるブロック暗号方式とは、ブロックの暗号化がそのブロックの前のブロックに依存する方式である。

【０００４】連鎖のあるブロック暗号方式の１例として、暗号文ブロック連鎖方式（ＣＢＣモード）について説明する。

【０００５】図９は、このような暗号文ブロック連鎖方式（ＣＢＣモード）を用いた従来のディジタルスクランブル伝送装置の構成図である。ここで、2aはスクランブル装置、2eはデスクランブル装置、2b，2fはＣＢＣレジスタ、2c，2gは排他的論理和回路、2dはブロック暗号化器、2hはブロック復号化器である。

【０００６】以上のように構成された従来例について、以下にその動作を説明する。スクランブル装置2aにおいて原信号$M_i$が入力される。スクランブル装置2aは、この原信号$M_i$を決まったビット数のブロックに分割し、ブロック単位でスクランブルを行う。スクランブルはスクランブル鍵をもとにブロック暗号化器2dで行われる。このようなブロックごとに分割し暗号化する方式がブロック暗号方式であるが、このとき、安全性を高めるために、以下に説明する暗号文ブロック連鎖方式（ＣＢＣモード）が用いられる。

【０００７】ＣＢＣレジスタ2bを用意しておき、このレジスタに１つ前のスクランブル装置2aの出力$C_{i-1}$を記憶するようにする。また、ＣＢＣ初期値には、スクランブル装置2aとデスクランブル装置2eに共通の値Ｖを準備

し、初期時にロードする。排他的論理和回路2cにおいて、ＣＢＣレジスタ2bの出力$C_{i-1}$と原信号$M_i$の排他的論理和の演算を行い、ブロック暗号化器2dに出力する。ブロック暗号化器2dは、排他的論理和回路2cからの信号を、スクランブル鍵をもとに暗号化を行い、スクランブル装置2aの出力としてスクランブル信号$C_i$を出力する。ブロック暗号化器2dで行われる暗号化の関数を$E_k$とすると、スクランブル信号$C_i$は、

$C_i = E_k$（$M_i$「＋」$C_{i-1}$）

と表すことができる。ここで、記号「＋」は排他的論理和を示す。

【０００８】一方、デスクランブル装置2eでは、スクランブル装置2aと逆の処理を行う。すなわち、ブロック復号化器2hにおいて、スクランブル信号$C_i$が決まったビット長のブロックに分割され、復号が行われる。このときブロック復号装置2hで行われる処理$D_k$は、ブロック暗号化器2dで行われる処理$E_k$の逆の処理であり、

$D_k$（$E_k$（$M_i$））$=M_i$

となるものである。

【０００９】以下、デスクランブル装置2eにおける暗号文ブロック連鎖方式（ＣＢＣモード）について説明する。

【００１０】ＣＢＣレジスタ2fにおいて、１つ前のスクランブル信号$C_{i-1}$を記憶し、排他的論理和回路2gに出力を行う。また、初期時には、スクランブル装置2aと共通の初期値ＶをＣＢＣレジスタ2fにロードする。ブロック復号化器2hは、スクランブル信号$C_i$を入力とし、スクランブル鍵をもとに復号を行い、排他的論理和回路2gに出力を行う。排他的論理和回路2gは、ＣＢＣレジスタ2fの出力$C_{i-1}$とブロック復号化器2hの出力$D_k$（$C_i$）の排他的論理和の演算を行い、デスクランブル装置2eの出力として出力する。このときブロック復号化器2hの処理を$D_k$とすると、復号信号は、

$D_k$（$C_i$）「＋」$C_{i-1}$$=M_i$「＋」$C_{i-1}$「＋」$C_{i-1}$$=M_i$

と表すことができ、原信号$M_i$となることが分かる。ここで、記号「＋」は排他的論理和を示す。

【００１１】

【発明が解決しようとする課題】しかしながら前記のような構成では、以下のような２つの課題があった。

【００１２】第１の課題は、映像信号や音声信号において、ブロック暗号を用いる場合に、撹拌の程度を制御する効果制御が困難であるという課題である。

【００１３】効果制御というのは、正規の受信者が高解像度の画像を視聴できることに加えて正規の受信者以外の受信者でも低解像度の画像を視聴できるようにすることである。入力信号が映像や音声の単に各画像の画素のサンプル値や各音声の音素のサンプル値を示す信号であれば、ＯＦＢモードと呼ばれるブロック暗号の方式を用いることにより疑似乱数を発生させ、疑似乱数の１と０のビット数の割合を制御することにより、正規の受信者以外が受信できる映像、音声信号の撹拌の程度を制御できる効果制御（低解像度の画像を表示すること）を行うことができるが、通常、ディジタル信号を伝送、記録する際には、高能率符号化を行うことが多く、このような高能率符号化された信号の場合には、数ビットの信号を反転するだけで他の部分も解読困難となり、撹拌の程度を制御する効果制御が困難である（画像がどのようなものであるか全く分からなくなる）という問題がある。

【００１４】本発明はかかる点に鑑み、高能率符号化された信号に対する効果制御を容易に実現可能なスクランブル伝送装置、およびそのスクランブル装置、デスクランブル装置を提供することを目的とする。

【００１５】第２の課題は、ＡＴＭネットワークなどのパケット廃棄が発生するネットワークにおけるセル廃棄による影響の伝搬の問題である。

【００１６】この課題の１つ目の例を図１０を用いて説明する。図１０はパケット廃棄による影響の伝搬の説明図である。図１０において、3a，3cは優先パケット、3b，3dは非優先パケットである。

【００１７】ＡＴＭ伝送（Ansynchronous Transfer Mode：非同期転送モード）などの伝送方式によって伝送を行った場合には、ネットワークにおいて非優先パケットの廃棄が行われるが、連鎖のある暗号を用いた場合、すなわち、スクランブルおよびデスクランブルが、対象となるブロックの前のブロックに依存した暗号方式を用いる場合に、非優先パケットの廃棄が行われたとき、そのパケットの次のパケットはデスクランブルが不可能となる。このように、パケット廃棄により非優先パケットの廃棄が行われた場合、次のパケットが復号できないため、そのパケットが重要なパケットである優先パケットであった場合には影響が大きいという問題がある。

【００１８】次に、図６を用いて、第２の課題の２つ目の例について説明する。図６はＭＰＥＧ　ｏｖｅｒ　ＡＴＭのＡＡＬ５による方式の説明図である。図６において、4a，4bはＭＰＥＧ２標準に準拠したトランスポートパケット、4cはＡＴＭ　ＡＡＬ５におけるＣＰＣＳ－ＰＤＵトレーラー、4d，4e，4f，4g，4h，4i，4j，4kはＡＴＭセルである。図６はＭＰＥＧ２のトランスポートパケットをＡＴＭセルで伝搬する際の方法を示すものであり、トランスポートパケット4a，4bの２つにＣＲＣを含むＣＰＣＳ－ＰＤＵトレーラー4cを加えたものを８つのＡＴＭセル4d，4e，4f，4g，4h，4i，4j，4kのペイロードに割り当てる。

【００１９】この例の場合、１つのＡＴＭセルが廃棄により失われると、そのＡＴＭセルを含むトランスポートパケット２つについてＣＲＣのチェックがエラーとなるため復号不可能となり、更にその次のトランスポートパケット１つがデスクランブル不可能となるため、３つのトランスポートパケットが失われることになる。このよ

うに、複数パケットを単位として処理している場合には、１つのパケット廃棄により失われるパケットの数が大きく、パケット廃棄の問題は大きい。

【００２０】本発明はかかる点に鑑み、パケット廃棄の影響の低減を実現可能なスクランブル伝送装置、およびそのスクランブル装置、デスクランブル装置、信号処理装置を提供することを目的とする。

【００２１】

【課題を解決するための手段】本発明に係るスクランブル伝送装置は、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、優先度に応じてスクランブルモードの切り換えを行ってスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、優先度に応じてスクランブルモードの切り換えを行ってデスクランブルを行うデスクランブル装置とから構成されていることを特徴としている。パケット廃棄に関する優先度によりスクランブルモードを変更することによって、効果制御を実現できるとともに、パケット廃棄に対する影響を低減することができる。

【００２２】また、本発明に係るスクランブル伝送装置は、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、優先度の高いパケットについてはスクランブルを行わず、優先度の低いパケットについてはスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、スクランブル鍵が存在する場合には優先度の低いパケットについてのみデスクランブルを行い、スクランブル鍵が存在しない場合には優先度の低いパケットを廃棄するデスクランブル装置とから構成されていることを特徴としている。スクランブル装置においてパケット廃棄に関する優先度が低いパケットのみをスクランブルし、デスクランブル装置において、スクランブル鍵が存在する場合、すなわち視聴などの契約を行っている場合にはデスクランブルを行い、スクランブル鍵が存在しない場合、すなわち視聴などの契約を行っていない場合にはデスクランブル不可能な優先度の低いパケットは廃棄する。このようにすることによって、正規の受信者は優先度の高いパケットと優先度の低いパケットの両方を復号することができ、正規の受信者以外の受信者は優先度の高いパケットのみを復号することができる。従って、例えば原信号がディジタル映像信号のような信号の場合に、優先度の高いパケットに画像の低解像度の情報を、優先度の低いパケットに画像の低解像度の情報に追加する高解像度の情報をそれぞれ割り当てることによって、正規の受信者以外の受信者も低解像度の画像を視聴することが可能な効果制御を実現することができる。

【００２３】また、本発明に係るスクランブル伝送装置は、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてデスクランブルを行うデスクランブル装置とから構成されていることを特徴としている。パケット廃棄に関する優先度の高いパケットと低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルすることによって、ネットワーク中で優先度の低いパケットの廃棄が行われた場合にでも、優先度の高いパケットに影響を及ぼさないようにすることが可能となり、パケット廃棄への影響を低減することができる。

【００２４】また、本発明に係るスクランブル伝送装置は、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、２つの連続するパケットを単位として処理し、２つのパケットのうち一方が優先度の高いパケットの場合には、両方とも優先度の高いパケットに書き換えて出力する信号処理装置と、信号処理装置からの信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてデスクランブルを行うデスクランブル装置とから構成されていることを特徴としている。２つずつの連続したパケットを単位として処理を行うスクランブル伝送装置において、２つのパケットのうち一方が優先度の高いパケットの場合に両方とも優先度の高いパケットに書き換え、優先度の高いパケット単位と優先度の低いパケット単位とを別々の連鎖のある暗号方式の系列としてスクランブルし、優先度の低いパケットの廃棄の影響を低減することができる。すなわち、優先度の低いパケットの廃棄が行われた場合も、同じパケット単位内には優先度の高いパケットは含まれないため、同じパケット単位内の優先度の高いパケットには影響がなく、優先度の高いパケット単位とは別の連鎖のある暗号方式の系列のため、次のパケット単位の優先度の高いパケットにも影響がない。

【００２５】

【発明の実施の形態】本発明に係る請求項１のスクランブル伝送装置は、スクランブル装置とデスクランブル装置とを具備し、前記スクランブル装置は、パケット廃棄に関する優先度に応じて異なるスクランブルモードでスクランブルを行うように構成され、前記デスクランブル装置は、前記スクランブル装置からのデータについて前記パケット廃棄に関する優先度に応じて前記異なるスクランブルモードでデスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度によりスクランブルモードを変更することによって、効果制御を実現できるとともに、パケット廃棄に対

する影響を低減することができる。

【００２６】本発明に係る請求項２のスクランブル伝送装置は、上記請求項１において、スクランブル装置が優先度判定装置と暗号化装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、前記パケット廃棄に関する優先度を判定し、前記暗号化装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号化装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきスクランブルを行うように構成されていることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【００２７】本発明に係る請求項３のスクランブル伝送装置は、上記請求項１において、デスクランブル装置が優先度判定装置と暗号解読装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、前記パケット廃棄に関する優先度を有するパケットの優先度を判定し、前記暗号解読装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号解読装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきデスクランブルを行うように構成されていることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【００２８】本発明に係る請求項４のスクランブル伝送装置は、上記請求項１において、スクランブル装置は、パケット廃棄に関する優先度が高優先度のパケットについてはスクランブルを行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはスクランブルを行うように構成されていることを特徴としている。

【００２９】優先度の高いパケットに画像の低解像度の情報を、優先度の低いパケットに画像の低解像度の情報に追加する高解像度の情報をそれぞれ割り当てることによって、正規の受信者以外の受信者も低解像度の画像を視聴することが可能な効果制御を実現できる。

【００３０】本発明に係る請求項５のスクランブル伝送装置は、上記請求項１において、デスクランブル装置は、スクランブル鍵を有する場合には、パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはデスクランブルを行い、かつ、前記スクランブル鍵を有しない場合には、前記パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケット廃棄に関する優先度が低優先度のパケットについては廃棄を行うように構成されていることを特徴としている。優先度の高いパケットに画像の低解像度の情報を、優先度の低いパケットに画像の低解像度の情報に追加する高解像度の情報をそれぞれ割り当てることによって、正規の受信者以外の受信者も低解像度の画像を視聴することが可能な効果制御を実現できる。

【００３１】本発明に係る請求項６のスクランブル伝送装置は、上記請求項１において、スクランブル装置は、連鎖のある暗号方式でスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度の高いパケットと低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルすることによって、ネットワーク中で優先度の低いパケットの廃棄が行われた場合にでも、優先度の高いパケットに影響を及ぼさないようにすることが可能となり、パケット廃棄への影響を低減することができる。

【００３２】本発明に係る請求項７のスクランブル伝送装置は、上記請求項１において、デスクランブル装置は、連鎖のある暗号方式でデスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてデスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度の高いパケットと低いパケットを別々の連鎖のある暗号方式の系列としてデスクランブルすることによって、ネットワーク中で優先度の低いパケットの廃棄が行われた場合にでも、優先度の高いパケットに影響を及ぼさないようにすることが可能となり、パケット廃棄への影響を低減することができる。

【００３３】本発明に係る請求項８のスクランブル伝送装置は、上記請求項１において、２つの連続するパケットを単位として処理を行い、２つのパケットのうち一方のパケットのパケット廃棄に関する優先度が高優先度のパケットの場合には２つのパケットの両方を高優先度のパケットに書き換えて出力する信号処理装置を付加していることを特徴としている。優先度の高いパケット単位と優先度の低いパケット単位とを別々の連鎖のある暗号方式の系列としてスクランブルし、優先度の低いパケットの廃棄の影響を低減することができる。

【００３４】本発明に係る請求項９のスクランブル伝送装置は、上記請求項１において、パケット廃棄に関する優先度が、ＭＰＥＧ２トランスポートストリームにおけるトランスポートパケットの優先度を示す１ビットのフラグtransport _priorityであることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【００３５】本発明に係る請求項１０のスクランブル装置は、パケット廃棄に関する優先度に応じて異なるスクランブルモードでスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度によりスクランブルモードを変更することによって、効果制御を実現できるとともに、パケット廃棄に対する影響を低減することができる。

【００３６】本発明に係る請求項１１のスクランブル伝送装置は、上記請求項１０において、優先度判定装置と暗号化装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、入力されたパケットの前記パケット廃棄に関する優先度を判定し、前記暗号化装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号化装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきスクランブルを行うように構成されていることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【００３７】本発明に係る請求項１２のスクランブル装置は、上記請求項１０において、パケット廃棄に関する優先度が高優先度のパケットについてはスクランブルを行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはスクランブルを行うように構成されていることを特徴としている。優先度の高いパケットに画像の低解像度の情報を、優先度の低いパケットに画像の低解像度の情報に追加する高解像度の情報をそれぞれ割り当てることによって、正規の受信者以外の受信者も低解像度の画像を視聴することが可能な効果制御を実現できる。

【００３８】本発明に係る請求項１３のスクランブル装置は、上記請求項１０において、連鎖のある暗号方式でスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度の高いパケットと低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルすることによって、ネットワーク中で優先度の低いパケットの廃棄が行われた場合にでも、優先度の高いパケットに影響を及ぼさないようにすることが可能となり、パケット廃棄への影響を低減することができる。

【００３９】本発明に係る請求項１４のスクランブル装置は、上記請求項１０において、パケット廃棄に関する優先度が、ＭＰＥＧ２トランスポートストリームにおけるトランスポートパケットの優先度を示す１ビットのフラグtransport __priorityであることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【００４０】本発明に係る請求項１５のデスクランブル装置は、パケット廃棄に関する優先度に応じて異なるスクランブルモードでデスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度によりスクランブルモードを変更することによって、効果制御を実現できるとともに、パケット廃棄に対する影響を低減することができる。

【００４１】本発明に係る請求項１６のデスクランブル装置は、上記請求項１５において、優先度判定装置と暗号解読装置とを具備し、前記優先度判定装置は、パケット廃棄に関する優先度を有するパケットを入力とし、入力されたパケットの前記パケット廃棄に関する優先度を判定し、前記暗号解読装置にパケットとスクランブルモード信号を出力するように構成され、前記暗号解読装置は、前記優先度判定装置からの前記スクランブルモード信号に基づきデスクランブルを行うように構成されていることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【００４２】本発明に係る請求項１７のデスクランブル装置は、上記請求項１５において、スクランブル鍵を有する場合には、パケット廃棄に関する優先度が高優先度のパケットについてはデスクランブルを行わず、前記パケット廃棄に関する優先度が低優先度のパケットについてはデスクランブルを行い、かつ、前記スクランブル鍵を有しない場合には、前記パケット廃棄に関する優先度が高優先度のパケットについては処理を行わず、前記パケットに関する優先度が低優先度のパケットについては廃棄を行うように構成されていることを特徴としている。優先度の高いパケットに画像の低解像度の情報を、優先度の低いパケットに画像の低解像度の情報に追加する高解像度の情報をそれぞれ割り当てることによって、正規の受信者以外の受信者も低解像度の画像を視聴することが可能な効果制御を実現できる。

【００４３】本発明に係る請求項１８のデスクランブル装置は、上記請求項１５において、連鎖のある暗号方式でデスクランブルを行い、パケット廃棄に関する優先度が高優先度のパケットと低優先度のパケットとを別々の前記連鎖のある暗号方式の系列としてデスクランブルを行うように構成されていることを特徴としている。パケット廃棄に関する優先度の高いパケットと低いパケットを別々の連鎖のある暗号方式の系列としてデスクランブルすることによって、ネットワーク中で優先度の低いパケットの廃棄が行われた場合にでも、優先度の高いパケットに影響を及ぼさないようにすることが可能となり、パケット廃棄への影響を低減することができる。

【００４４】本発明に係る請求項１９のデスクランブル装置は、上記請求項１５において、パケット廃棄に関する優先度が、ＭＰＥＧ２トランスポートストリームにおけるトランスポートパケットの優先度を示す１ビットのフラグtransport __priorityであることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【００４５】本発明に係る請求項２０のスクランブル伝送装置用の信号処理装置は、パケット廃棄に関する優先度を有するパケットを入力とし、入力された２つの連続するパケットを単位として処理を行い、２つのパケットのうち一方のパケットのパケット廃棄に関する優先度が高優先度のパケットの場合には２つのパケットの両方を高優先度のパケットに書き換えてスクランブル装置に出

力するように構成されていることを特徴としている。２つずつの連続したパケットを単位として処理を行うスクランブル伝送装置において、優先度の低いパケットの廃棄が行われた場合も、同じパケット単位内には優先度の高いパケットは含まれないため、同じパケット単位内の優先度の高いパケットには影響がなく、優先度の高いパケット単位とは別の連鎖のある暗号方式の系列のため、次のパケット単位の優先度の高いパケットにも影響がない。

【００４６】本発明に係る請求項２１のスクランブル伝送装置用の信号処理装置は、パケット廃棄に関する優先度が、ＭＰＥＧ２トランスポートストリームにおけるトランスポートパケットの優先度を示す１ビットのフラグtransport __priorityであることを特徴としている。効果制御を実現できるとともに、パケット廃棄に対する影響を低減できる。

【００４７】本発明に係る請求項２２のスクランブル装置は、上記請求項８において、２つの連続するパケットを単位として処理を行うことに代えて、３つ以上の連続するパケットを単位として処理を行うように構成してあることを特徴としている。効果制御とパケット廃棄影響低減の効果に拡張性をもたせることができる。

【００４８】本発明に係る請求項２３のスクランブル伝送装置用の信号処理装置は、上記請求項２０において、２つの連続するパケットを単位として処理を行うことに代えて、３つ以上の連続するパケットを単位として処理を行うように構成してあることを特徴としている。効果制御とパケット廃棄影響低減の効果に拡張性をもたせることができる。

【００４９】以下、本発明の実施の形態に係るスクランブル伝送装置について図面に基づいて詳細に説明する。

【００５０】〔実施の形態１〕図１は本発明の実施の形態１に係るスクランブル伝送装置の構成を示すブロック図である。

【００５１】図１において、1aはデータの符号化を行う符号化装置、1bは原信号を入力とし、優先度の書き換えを行う信号処理装置、1cは信号処理装置1bからの信号とスクランブル鍵を入力とし、パケットの優先度に応じてスクランブルを行い出力するスクランブル装置、1dはパケットの優先度からスクランブルモードを決定し、スクランブルモード信号と原信号を出力する優先度判定装置、1eはスクランブル鍵と優先度判定装置1dからのスクランブルモード信号に基づき原信号をスクランブルする暗号化装置、1fはスクランブル信号をＡＴＭセルに変換し、ＡＴＭネットワーク上に出力するＡＴＭアダプター、1gはネットワークからのＡＴＭセルをもとのスクランブル信号に戻すＡＴＭアダプター、1hはスクランブル信号をデスクランブルし、原信号に戻すデスクランブル装置、1iはスクランブル信号の優先度とスクランブル鍵からスクランブルモードを決定し、スクランブルモード信号とスクランブル信号を出力する優先度判定装置、1jはスクランブル鍵と優先度判定装置1iからのスクランブルモード信号に基づきスクランブル信号をデスクランブルする暗号解読装置、1kは符号化データの復号を行う復号化装置である。

【００５２】以上のように構成された本実施の形態１のスクランブル伝送装置において、以下にその動作を説明する。

【００５３】原信号はＭＰＥＧ(Moving Picture Expert Group：国際標準化機構ISO と国際電気標準会議IEC の合同の作業グループ）標準の映像信号をＭＰＥＧシステムのトランスポートパケットにより多重化し、Ｉピクチャーに対応するトランスポートパケットをtransport __priority＝１とし、ＰピクチャーおよびＢピクチャーに対応するトランスポートパケットのtransport __priority＝０とした信号であるとする。ＭＰＥＧ標準の詳細については、「最新ＭＰＥＧ教科書」（アスキー出版局編）にその解説がなされている。

【００５４】以下に、ＭＰＥＧ標準に基づく映像信号のピクチャーの構成およびＭＰＥＧシステム層におけるトランスポートストリームについて説明する。

【００５５】図２は、ＭＰＥＧ標準に準処した映像信号のピクチャーの構造の説明図である。以下、ＭＰＥＧ標準におけるピクチャーの構造について説明する。図２において、5a，5eがＩピクチャー、5b，5dがＢピクチャー、5cがＰピクチャーである。

【００５６】図２のようにＭＰＥＧ標準に準拠した映像信号は、３つのピクチャー、すなわち、Ｉピクチャー、Ｐピクチャー、Ｂピクチャーに分けられる。Ｉピクチャー5a，5eは、その情報からだけで符号化された画面で、フレーム間予測を使わずに生成される。Ｐピクチャー5cは、ＩピクチャーまたはＰピクチャーからの順方向予測を行うことによってできる画面で、単独では復号することはできない。Ｂピクチャー5b，5dは、過去のＩピクチャーまたはＰピクチャーからの順方向予測と未来のＩピクチャーまたはＰピクチャーからの逆方向予測とを合わせた双方向予測を行うことによってできる画面で、単独では復号することはできない。

【００５７】以下、ＭＰＥＧ標準のシステムストリームにおけるトランスポートストリームについて説明する。図３は、ＭＰＥＧ標準に準処したトランスポートパケットの構成図である。図３において、6aはトランスポートパケットである。トランスポートストリームは、長さ１８８byteのトランスポートパケット6aからなり、トランスポートパケット6aは、基本的に４byteのヘッダと、１８４byteのペイロードからなる。

【００５８】次に、トランスポートパケットヘッダ中のシンタックスについて説明する。まず、ＰＩＤは、ペイロードに含まれる情報の区別を行い、このシンタックスにより、映像信号か音声信号かなどの判別が可能とな

15

る。また、transport __priorityは、そのトランスポートの優先度を示す1bit のフラグであり、次に述べるＡＴＭ伝送への対応などの目的に用いられる。また、transport __scrambling__control によりパケットにスクランブルかかかっているかどうかなどのパケットのスクランブル情報が示される。

【００５９】ネットワーク上の伝送方式としては、ＡＴＭ（Ansynchronous Transfer Mode：非同期転送モード）伝送を用い、ＡＴＭセル上にＭＰＥＧ信号を割り当てる方式としてＭＰＥＧ　ｏｖｅｒ　ＡＴＭを用いるものとする。ＡＴＭ伝送およびＭＰＥＧ　ｏｖｅｒ　ＡＴＭの詳細については、「標準ＡＴＭ教科書」（アスキー出版局編）にその解説がなされている。

【００６０】以下に、ＡＴＭ伝送について説明する。

【００６１】図４はＡＴＭ伝送で用いられるＡＴＭセルの構成図である。図４において、7aはＡＴＭセルである。ＡＴＭ伝送では、情報をＡＴＭセルと呼ばれる固定長のセルに分解して伝送することにより高速伝送を実現する。ＡＴＭセルは、図４に示すとおり５３byteの固定長であり、５byteのヘッダと４８byteのペイロードをもつ。ＡＴＭ伝送においては、原理上、セル廃棄すなわちネットワーク上で輻輳などのためセルを廃棄する必要が生じることがあるが、この際、ヘッダ中のCell Loss Priorityが用いられる。Cell Loss Priorityは、1bit のシンタックスで、セルが高優先であるか低優先であるかを示す。ＡＴＭネットワークでは、セル廃棄の必要が生じた場合には、このCell Loss Priorityを見て、優先度の低いセルを先に廃棄するようにする。

【００６２】次に、ＭＰＥＧ　ｏｖｅｒ　ＡＴＭについて説明する。ＭＰＥＧ　ｏｖｅｒＡＴＭとは、先に説明したＭＰＥＧ標準におけるトランスポートストリームのトランスポートパケットをＡＴＭ伝送で伝送する際の方式である。ＭＰＥＧ　ｏｖｅｒ　ＡＴＭの方式としては現在、ＡＡＬ１，ＡＡＬ５の２つの方式が考えられている。以下、ＡＡＬ１，ＡＡＬ５の２つのＭＰＥＧ　ｏｖｅｒ　ＡＴＭの方式について説明する。

【００６３】図５はＡＡＬ１によるＭＰＥＧ　ｏｖｅｒ　ＡＴＭの方式の説明図である。図５において、8aはトランスポートパケット、8b，8c，8d，8eはＡＴＭセルである。図５に示すように、ＡＡＬ１では、１８８byteのトランスポートパケット8aを４７byteのブロック４つに分割し、ＡＴＭセル8b，8c，8d，8eのペイロードに配置する。

【００６４】また、ＡＡＬ５によるＭＰＥＧ　ｏｖｅｒ　ＡＴＭの方式では、図６で示したように、ＭＰＥＧのトランスポートパケット4a，4bの２つを単位として、これにＣＲＣを含むＣＰＣＳ－ＰＤＵトレーラー4cを加えたものを８つのＡＴＭセル4d，4e，4f，4g，4h，4i，4j，4kのペイロードに割り当てる。

【００６５】また、暗号方式としては、暗号文ブロック連鎖方式（ＣＢＣモード）を用いる。

16

【００６６】以上のような原信号、伝送方式、暗号方式を扱う本実施の形態１について、図１に戻って以下にその動作を説明する。

【００６７】送信側では、データの符号化、スクランブル、送信を行う。

【００６８】まず、符号化装置1aにおいて、ＭＰＥＧ準拠の映像信号を生成し、Ｉピクチャーに対応するデータをパケット廃棄に関する優先度の高いトランスポートパケットとして、すなわちtransport __priority＝１のトランスポートパケットとして、また、ＰピクチャーおよびＢピクチャーに対応するデータをパケット廃棄に関する優先度の低いトランスポートパケットとして、すなわちtransport __priority＝０のトランスポートパケットとして、信号処理装置1bに出力する。

【００６９】実施の形態１においては、信号処理装置1bでは、処理を行わず、符号化装置1aからの原信号をそのまま出力する。

【００７０】信号処理装置1bからの信号を受けとったスクランブル装置1cでは、優先度の低いパケットに対してスクランブルを行う。信号は、まず、優先度判定装置1dに入力され、ここで、トランスポートパケット中のtransport __priorityを見て、０の場合にはスクランブルを行うスクランブルモード信号を、１の場合にはスクランブルを行わないスクランブルモード信号を暗号化装置1eに出力する。暗号化装置1eでは、スクランブルモード信号とスクランブル鍵に基づきトランスポートパケット単位に処理を行う。スクランブルモード信号がスクランブルを示す信号の場合には、スクランブル鍵に基づきトランスポートパケットのスクランブルを行い、スクランブルモード信号がノンスクランブルを示す信号の場合にはトランスポートパケットをそのまま出力する。

【００７１】ＡＴＭアダプター1fでは、スクランブル装置1cからのトランスポートパケットをＡＴＭセルに変換し出力する。図５に示すＭＰＥＧ　ｏｖｅｒ　ＡＴＭのＡＡＬ１を用いて、トランスポートパケットを４つのＡＴＭセルに分割して送信を行う。この際、ＡＴＭアダプター1fでは、transport __priority＝１のトランスポートパケットはCell Loss Priority＝１のＡＴＭセルとして、transport __priority＝０のトランスポートパケットはCell Loss Priority＝０のＡＴＭセルとして出力する。

【００７２】次に、受信側の動作について説明する。受信側では、受信、デスクランブル、データの復号化を行う。

【００７３】ＡＴＭアダプター1gでは、ネットワークからのＡＴＭセルをトランスポートパケットに変換する。図５に示すＭＰＥＧ　ｏｖｅｒ　ＡＴＭのＡＡＬ１を用い、分割した４つのＡＴＭセルを１つのトランスポートパケットに戻し、トランスポートパケットを出力する。

この際、ＡＴＭアダプター1gでは、Cell Loss Priority＝１のＡＴＭセルはtransport __priority＝１のトランスポートパケットとして、Cell Loss Priority＝０のＡＴＭセルはtransport __priority＝０のトランスポートパケットとして出力する。

【００７４】次に、デスクランブル装置1hでは、契約を行っていて視聴可能な場合には、優先度の低いパケットについてはデスクランブルを行い、優先度の高いパケットは処理を行わずそのまま出力する。契約を行っておらず視聴不可の場合には、優先度の低いパケットは削除して、優先度の高いパケットのみ処理せずにそのまま出力する。スクランブルされたトランスポートパケットを入力した優先度判定装置1iでは、契約を行っていて視聴可能な場合（スクランブル鍵が存在する場合）には、transport __priorityを見て、transport __priority＝１の場合はスクランブルモード信号を処理しないモードに、transport __priority＝０の場合はスクランブルモード信号をデスクランブルするモードにし、契約を行っておらず視聴不可能な場合（スクランブル鍵が存在しない場合）には、transport __priority＝１の場合はスクランブルモード信号を処理しないモードに、transport __priority＝０の場合はスクランブルモード信号をパケット廃棄を行うモードにして出力する。暗号解読装置1jでは、スクランブルモード信号を見て、スクランブルモード信号が処理しないモードの場合にはトランスポートパケットの処理は行わず、スクランブルモード信号がデスクランブルモードの場合にはスクランブル鍵をもとにデスクランブルを行い、スクランブルモード信号がパケット廃棄の場合にはトランスポートパケットをＮＵＬＬパケットに置き換えて出力する。

【００７５】復号化装置1kは、デスクランブル装置1hの出力を受け取り、データの復号を行う。

【００７６】以上のような動作により、本実施の形態１では、正規の受信者は、Ｉピクチャー、Ｐピクチャーおよびピクチャーのすべてのピクチャーを復号することが可能となり、正常の動画像を得ることができる。また、正規の受信者以外の受信者は、優先度の高いトランスポートパケットのみを得て、Ｉピクチャーのみを復号することが可能となり、正規の受信者以外もある程度の画像を得ることのできる効果制御を実現できる。

【００７７】また、本実施の形態１においては、優先度を示す１ビットのフラグtransport__priorityをスクランブルのＯＮ／ＯＦＦの制御に用いることができるため、2bit のシンタックスtransport __scrambling__control をＯＮ／ＯＦＦ以外の制御に2bit 使うことができるという利点もある。

【００７８】なお、スクランブル鍵は公知の手段で伝送を行うことができる。

【００７９】また、本実施の形態１では、符号化装置1aでの優先度の割り当ての方法として、Ｉピクチャーを優先度の高いパケットに、Ｐピクチャーおよびピクチャーを優先度の低いパケットに割り当てる方法を１例として挙げたが、優先度の高いパケットに対応する情報が単独で復号可能な他のいかなる割り当て法でも効果制御を実現することができる。他の例としては、階層符号化方式であるＭＰＥＧのスケーラビリティーを用いて、高位レイヤの画像を優先度の低いトランスポートパケットに、低位レイヤの画像を優先度の高いトランスポートパケットに割り当て、正規の受信者以外が低位レイヤの画像のみを視聴することができるようにする方法や、ＤＣＴ（離散コサイン変換）成分の交流成分の情報を優先度の低いトランスポートパケットに、それ以外の情報を優先度の高いトランスポートパケットに割り当てることにより、正規の受信者以外が直流成分のみを含むモザイク状の画像を視聴することができるようにする方法などがある。また、本方式がＭＰＥＧ以外のパケット廃棄に関する優先度を含む信号を出力する映像、音声などのデータ信号すべてに対して有効であることはいうまでもない。

【００８０】なお、本実施の形態１では、ネットワークの伝送方法として、ＡＴＭ（非同期転送モード）による伝送の例を挙げたが、他のいかなる伝送方法においてもまた記録メディアにおいても、本発明は有効である。

【００８１】また、本実施の形態１では、暗号方式として、暗号化ブロック連鎖方式（ＣＢＣモード）を例として挙げたが、他のいかなる暗号方式においても、本発明は有効である。

【００８２】〔実施の形態２〕次に、本発明の実施の形態２に係るスクランブル伝送装置について説明する。

【００８３】実施の形態２の説明においては、実施の形態１の説明で用いた図１を利用する。

【００８４】原信号はＭＰＥＧ標準の映像信号をＭＰＥＧシステムのトランスポートパケットにより多重化し、Ｉピクチャーに対応するトランスポートパケットをtransport __priority＝１、Ｐピクチャーおよびピクチャーに対応するトランスポートパケットをtransport __priority＝０とした信号であるとする。次に、ネットワーク上の伝送方式としてはＡＴＭ伝送を用い、ＡＴＭセル上にＭＰＥＧ信号を割り当てる方式としてＭＰＥＧ ｏｖｅｒ ＡＴＭのＡＡＬ１（図５参照）を用いるものとする。また、暗号方式としては暗号文ブロック連鎖方式（ＣＢＣ）を用いる。

【００８５】以上のような原信号、伝送方式、暗号方式を扱う本実施の形態２について、図１を用いて以下にその動作を説明する。

【００８６】送信側では、データの符号化、スクランブル、送信を行う。

【００８７】まず、符号化装置1aにおいて、ＭＰＥＧ準拠の映像信号を生成し、Ｉピクチャーに対応するデータをパケット廃棄に関する優先度の高いトランスポートパ

ケットとして、すなわちtransport _priority＝１のトランスポートパケットとして、Ｐピクチャーおよびピクチャーに対応するデータをパケット廃棄に関する優先度の低いトランスポートパケットとして、すなわちtransport _priority＝０のトランスポートパケットとして信号処理装置1bに出力する。

【００８８】実施の形態２においては、信号処理装置1bでは処理を行わず、符号化装置1aからの原信号をそのまま出力する。

【００８９】信号処理装置1bからの信号を受け取ったスクランブル装置1cでは、優先度の高いパケットと優先度の低いパケットとを別々の連鎖のある暗号方式の系列としてスクランブルを行う。この動作を図７を用いて説明する。図７において、9a，9c，9eは優先度の高いパケット、9b，9dは優先度の低いパケットである。暗号化装置1eは、優先度の高いパケットと優先度の低いパケットのそれぞれに対するＣＢＣレジスタを用意するものし、図７に示すように、優先度の高いパケットのスクランブルを行うときには、前の優先度の高いパケットのＣＢＣレジスタの値を用いてスクランブルを行い（ＣＢＣ系列２）、優先度の低いパケットのスクランブルを行うときには、前の優先度の低いパケットのＣＢＣレジスタの値を用いてスクランブルを行う（ＣＢＣ系列１）ことによって、優先度の高いパケットと優先度の低いパケットを別々の系列の連鎖のある暗号方式としてスクランブルを行う。スクランブル装置1cに入力された原信号は、優先度判定装置1dに入力され、ここで、トランスポートパケット中のtransport _priorityを見て、１の場合には優先度の高いパケットを示すスクランブルモード信号を、０の場合には優先度の低いパケットを示すスクランブルモード信号を暗号化装置1eに出力する。暗号化装置1eでは、スクランブルモード信号とスクランブル鍵に基づきトランスポートパケット単位に処理を行う。スクランブルモード信号が優先度の高いパケットを示す信号の場合には、優先度の高いパケット用のＣＢＣレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式（ＣＢＣモード）でトランスポートパケットのスクランブルを行い、スクランブルモードが優先度の低いパケットの場合には、優先度の低いパケット用のＣＢＣレジスタを用いて、スクランブル鍵に基づき暗号文ブロック暗号方式でトランスポートパケットのスクランブルを行う。また、この際、スクランブル装置1cは、transport _scrambling_controlをＯＮにして出力を行う。

【００９０】ＡＴＭアダプター1fでは、スクランブル装置1cからのトランスポートパケットをＡＴＭセルに変換し、出力する。図５に示すＭＰＥＧ　ｏｖｅｒ　ＡＴＭのＡＡＬ１を用いてトランスポートパケットを４つのＡＴＭセルに分割し、送信を行う。この際、ＡＴＭアダプター1fでは、transport _priority＝１のトランスポートパケットはCell Loss Priority＝１のＡＴＭセルとして、transport _priority＝０のトランスポートパケットはCell Loss Priority＝０のＡＴＭセルとして出力する。

【００９１】次に、受信側の動作について説明する。受信側では、受信、デスクランブル、データの復号化を行う。

【００９２】ＡＴＭアダプター1gでは、ネットワークからのＡＴＭセルをトランスポートパケットに変換する。図５に示すＭＰＥＧ　ｏｖｅｒ　ＡＴＭのＡＡＬ１を用い、分割した４つのＡＴＭセルを１つのトランスポートパケットに戻し、トランスポートパケットを出力する。この際、ＡＴＭアダプター1gでは、Cell Loss Priority＝１のＡＴＭセルはtransport _priority＝１のトランスポートパケットとして、Cell Loss Priority＝０のＡＴＭセルはtransport _priority＝０のトランスポートパケットとして出力する。

【００９３】この信号を受け取ったデスクランブル装置1hでは、図７に示したように優先度の高いパケットと優先度の低いパケットとを別々の連鎖のある暗号方式の系列としてデスクランブルを行う。デスクランブル装置1hに入力された信号は、優先度判定装置1iに入力され、ここで、トランスポートパケット中のtransport _priorityを見て、１の場合には優先度の高いパケットを示すスクランブルモード信号を、０の場合には優先度の低いパケットを示すスクランブルモード信号を暗号解読装置1jに出力する。暗号解読装置1jでは、スクランブルモード信号とスクランブル鍵に基づきトランスポートパケット単位に処理を行う。スクランブルモード信号が優先度の高いパケットを示す信号の場合には、優先度の高いパケット用のＣＢＣレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式（ＣＢＣモード）でトランスポートパケットのデスクランブルを行い、スクランブルモード信号が優先度の低いパケットの場合には、優先度の低いパケット用のＣＢＣレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式（ＣＢＣモード）でトランスポートパケットのデスクランブルを行う。また、この際、デスクランブル装置1hは、transport _scrambling_control をＯＦＦにして出力を行う。

【００９４】復号化装置1kは、デスクランブル装置1hの出力を受け取り、データの復号を行う。

【００９５】以上のような動作により、この実施の形態２では、パケットの廃棄に対する影響を低減したスクランブル伝送装置を実現することができる。すなわち、ＡＴＭネットワーク上でセル廃棄が行われた場合に、優先度の異なるトランスポートパケットを同じ連鎖のある暗号方式の系列としてスクランブルを行った場合には、図１０で示したように、次の優先度の高いパケットがデスクランブルできない可能性がある。しかしながら、本実施の形態２のようなスクランブル伝送装置によれば、優先度の低いパケットが廃棄された場合にも、優先度の高

いパケットがデスクランブルできない可能性はなくなり、パケット廃棄の影響を低減したスクランブル伝送装置を実現できる。本実施の形態２のように、Ｉピクチャーに対応するデータをパケット廃棄に関する優先度の高いトランスポートパケットとし、ＰピクチャーおよびＢピクチャーに対応するデータをパケット廃棄に関する優先度の低いトランスポートパケットとした場合には、相対的に重要な情報であるＩピクチャーのデータは失われないため、ＡＴＭネットワークにおいてパケット廃棄が行われた場合にも、乱れの少ない画像を受信者は視聴することができる。

【００９６】なお、スクランブル鍵は公知の手段で伝送を行うことができる。

【００９７】また、本実施の形態２では、符号化装置1aでの優先度の割り当ての方法として、Ｉピクチャーを優先度の高いパケットに、ＰピクチャーおよびＢピクチャーを優先度の低いパケットに割り当てる方法を１例として挙げたが、他のいかなる割り当て法においても本発明は有効である。更に、本方式がＭＰＥＧ以外のパケット廃棄に関する優先度をもつ信号を出力する映像、音声などのデータ信号すべてに有効であることはいうまでもない。

【００９８】なお、本実施の形態２では、ネットワークの伝送方法としてＡＴＭ（非同期転送モード）による伝送の例を挙げたが、他のいかなるパケット廃棄が行われる伝送方法においてもまた記録メディアにおいても、本発明は有効である。

【００９９】また、本実施の形態２では、暗号方式として、暗号文ブロック連鎖方式（ＣＢＣモード）を例として挙げたが、他のいかなる連鎖のある暗号方式においても、本発明は有効である。

【０１００】〔実施の形態３〕次に、本発明の実施の形態３に係るスクランブル伝送装置ついて説明する。実施の形態３の説明においては、実施の形態１の説明で用いた図１を利用する。

【０１０１】原信号はＭＰＥＧ標準の映像信号をＭＰＥＧシステムのトランスポートパケットにより多重化し、Ｉピクチャーに対応するトランスポートパケットをtransport __priority＝１とし、ＰピクチャーおよびＢピクチャーに対応するトランスポートパケットをtransport __priority＝０とした信号であるとする。次に、ネットワーク上の伝送方式としては、ＡＴＭ伝送を用い、ＡＴＭセル上にＭＰＥＧ信号を割り当てる方式としてＭＰＥＧ　ｏｖｅｒ　ＡＴＭのＡＡＬ５を用いるものとする。また、暗号方式としては、暗号文ブロック連鎖方式（ＣＢＣモード）を用いる。

【０１０２】以上のような原信号、伝送方式、暗号方式を扱う本実施の形態３について、図１を用いて以下にその動作を説明する。

【０１０３】送信側では、データの符号化、スクランブル、送信を行う。

【０１０４】まず、符号化装置1aにおいて、ＭＰＥＧ準拠の映像信号を生成し、Ｉピクチャーに対応するデータをパケット廃棄に関する優先度の高いトランスポートパケットとして、すなわちtransport __priority＝１のトランスポートパケットとして、また、ＰピクチャーおよびＢピクチャーに対応するデータをパケット廃棄に関する優先度の低いトランスポートパケットとして、すなわちtransport __priority＝０のトランスポートパケットとして信号処理装置1bに出力する。

【０１０５】次に、この信号処理装置1bからの信号を、送信側でどのように処理するかを以下に図８を用いて説明する。図８において、10a，10e，10f，10i，10m，10n，10q，10r，10u，10v は優先度の高い優先パケット、10b，10c，10d，10g，10h，10j，10k，10l，10o，10p，10s，10t，10w，10x は優先度の低い非優先パケットである。図８に示すように、パケットは２つを単位として処理が行われ、信号処理装置1bにおいて、優先度の高いパケットを１つ含むパケット単位は、両方のパケットが優先度の高いパケットに書き換えられる。

【０１０６】次にスクランブル装置1cにおいては、優先度の高いパケット単位は、優先度の高いパケットを含む前のパケット単位の系列（ＣＢＣ系列２）のＣＢＣレジスタの値を用いてスクランブルが行われ、優先度の高いパケットを含まないパケット単位は、前の優先度の高いパケットを含まないパケット単位の系列（ＣＢＣ系列１）のＣＢＣレジスタの値を用いてスクランブルが行われる。以上のような動作により、送信側では、優先度の高いパケットを含むパケット単位と優先度の高いパケットを含まないパケット単位を、別々の系列の暗号文ブロック連鎖方式（ＣＢＣモード）としてスクランブルを行う。

【０１０７】符号化装置1aからの原信号を受け取った信号処理装置1bでは、２つのトランスポートパケット単位に処理を行い、トランスポートパケット２つのうち一方が優先度の高いパケットの場合には、２つとも優先度の高いパケットに書き換える。

【０１０８】この様子が図８に示されている。例えば、優先パケット10a と非優先パケット10b とからなるパケット単位ではそれぞれが優先パケット10m と優先パケット10nになる。また、優先パケット10e と優先パケット10f とからなるパケット単位ではそれぞれがもとと同じ優先パケット10q と優先パケット10r になる。また、非優先パケット10c と非優先パケット10d とからなるパケット単位ではそれぞれがもとと同じ非優先パケット10o と非優先パケット10p になる。

【０１０９】信号処理装置1bからの信号を受け取ったスクランブル装置1cでは、優先度の高いパケットと優先度の低いパケットとを別々の暗号文ブロック連鎖方式（Ｃ

ＢＣモード）の系列としてスクランブルを行う。スクランブル装置1cに入力された信号は優先度判定装置1dに入力され、トランスポートパケット中のtransport __priorityを見て、１の場合には優先度の高いパケットを示すスクランブルモード信号を、０の場合には優先度の低いパケットを示すスクランブルモード信号を暗号化装置1eに出力する。暗号化装置1eでは、スクランブルモード信号とスクランブル鍵に基づきトランスポートパケット単位に処理を行う。スクランブルモード信号が優先度の高いパケットを示す信号の場合には、優先度の高いパケット用のＣＢＣレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式（ＣＢＣモード）でトランスポートパケットのスクランブルを行い、スクランブルモードが優先度の低いパケットの場合には、優先度の低いパケット用のＣＢＣレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式でトランスポートパケットのスクランブルを行う。また、この際、スクランブル装置1cは、transport __scrambling__control をＯＮにして出力を行う。

【０１１０】ＡＴＭアダプター1fは、スクランブル装置1cからのスクランブルされたトランスポートパケットをＡＴＭセルに変換し、出力する。図６に示すＭＰＥＧ ｏｖｅｒ ＡＴＭのＡＡＬ５を用いて、単位となっているトランスポートパケット２つとＣＲＣなどを含むＣＰＣＳ－ＰＤＵトレーラーを、ＡＴＭセル８つに分割して送信を行う。この際、ＡＴＭアダプター1fでは、transport __priority＝１のトランスポートパケットはCell Loss Priority＝１のＡＴＭセルとして、transport __priority＝０のトランスポートパケットはCell Loss Priority＝０のＡＴＭセルとして出力する。

【０１１１】次に、受信側の動作について説明する。受信側では、受信、デスクランブル、データの復号化を行う。

【０１１２】ＡＴＭアダプター1gでは、ネットワークからのＡＴＭセルをトランスポートパケットに変換する。図６に示すＭＰＥＧ ｏｖｅｒ ＡＴＭのＡＡＬ５を用い、分割した８つのＡＴＭセルを２つのトランスポートパケットに戻し、トランスポートパケットを出力する。この際、ＡＴＭアダプター1gでは、Cell Loss Priority＝１のＡＴＭセルはtransport __priority＝１のトランスポートパケットとして、Cell Loss Priority＝０のＡＴＭセルはtransport __priority＝０のトランスポートパケットとして出力する。

【０１１３】この信号を受け取ったデスクランブル装置1hでは、図８に示したように優先度の高いパケットと優先度の低いパケットとを別々の連鎖のある暗号方式の系列としてデスクランブルを行う。デスクランブル装置1hに入力されたスクランブル信号は優先度判定装置1iに入力され、ここでトランスポートパケット中のtransport __priorityを見て、１の場合には優先度の高いパケットを示すスクランブルモード信号を、０の場合には優先度の低いパケットを示すスクランブルモード信号を暗号解読装置1jに出力する。暗号解読装置1jでは、スクランブルモード信号とスクランブル鍵に基づきトランスポートパケット単位に処理を行う。スクランブルモード信号が優先度の高いパケットを示す信号の場合には、優先度の高いパケット用のＣＢＣレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式（ＣＢＣモード）でトランスポートパケットのデスクランブルを行い、スクランブルモードが優先度の低いパケットの場合には、優先度の低いパケット用のＣＢＣレジスタを用いて、スクランブル鍵に基づき暗号文ブロック連鎖方式でトランスポートパケットのデスクランブルを行う。また、この際、デスクランブル装置1hは、transport __scrambling __control をＯＦＦにして出力を行う。

【０１１４】復号化装置1kは、デスクランブル装置1hの出力を受け取り、データの復号を行う。

【０１１５】以上のような動作により、この実施の形態３では、ＭＰＥＧ ｏｖｅｒ ＡＴＭのＡＡＬ５などのように複数パケットを単位としてネットワークにおける伝送を行う場合に、パケットの廃棄に対する影響を低減したスクランブル伝送装置を実現することができる。すなわち、これまでは、ＡＴＭネットワーク上で優先度の低いセルの廃棄が行われた場合、そのＡＴＭセルを含むトランスポートパケットは復号不可能となり、従って、ＡＡＬ５でそのトランスポートパケットとペアになっていたトランスポートパケットも復号不可能となる。更に暗号文ブロック連鎖方式（ＣＢＣモード）を用いている場合には、同じ連鎖上の次のトランスポートパケットも復号不可能となる。しかし、本実施の形態３におけるスクランブル伝送装置では、優先度の低いセルが廃棄され、そのセルを含むトランスポートパケットが復号不可能となった場合にも、ＡＡＬ５上でペアとなっているトランスポートパケットは優先度の低いトランスポートパケットであり、連鎖上で次のトランスポートパケットも優先度の低いパケットであるため、影響が少ないという効果がある。

【０１１６】本実施の形態３のように、Ｉピクチャーに対応するデータをパケット廃棄に関する優先度の高いトランスポートパケットとし、ＰピクチャーおよびＢピクチャーに対応するデータをパケット廃棄に関する優先度の低いトランスポートパケットとした場合には、相対的に重要な情報であるＩピクチャーのデータは失われないため、パケット廃棄が行われた場合にも、乱れの少ない画像を受信者は視聴することができる。

【０１１７】なお、スクランブル鍵は公知の手段で伝送を行うことができる。

【０１１８】また、本実施の形態３では、符号化装置1aでの優先度の割り当ての方法として、Ｉピクチャーを優先度の高いパケットに、ＰピクチャーおよびＢピクチャ

ーを優先度の低いパケットに割り当てる方法を１例として挙げたが、他のいかなる割り当て法に対しても本発明は有効である。更に、本方式がＭＰＥＧ以外のパケット廃棄に関する優先度をもつ信号を出力する映像、音声などのデータ信号すべてに有効であることはいうまでもない。

【０１１９】なお、本実施の形態３では、ネットワークの伝送方法としてＡＴＭ（非同期転送モード）による伝送の例を挙げたが、他のいかなるパケット廃棄が行われる伝送方法においてもまた記録メディアにおいても、本発明は有効である。

【０１２０】また、本実施の形態３では、暗号方式として、暗号文ブロック連鎖方式（ＣＢＣモード）を例として挙げたが、他のいかなる連鎖のある暗号方式においても、本発明は有効である。

【０１２１】なお、本実施の形態３では、符号化装置1aの出力するパケットを２つ単位で処理してネットワーク中の伝送するＭＰＥＧ　ｏｖｅｒ　ＡＴＭのＡＡＬ５を例として挙げたが、２つ以上の単位でパケットを処理するいかなる処理に対しても、本発明は有効である。

【０１２２】更に、本発明の他の実施の形態としては、符号化装置の処理速度に比べて、スクランブル装置、デスクランブル装置の処理速度が遅く、すべてのパケットの処理を行うことができない場合に、優先度を用いて、高優先のパケットのみをスクランブルする実施の形態などが考えられ、本発明の実用的意義は大きい。

【０１２３】

【発明の効果】本発明に係るスクランブル伝送装置によれば、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、優先度に応じてスクランブルモードの切り換えを行ってスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、優先度に応じてスクランブルモードの切り換えを行ってデスクランブルを行うデスクランブル装置とから構成されており、パケット廃棄に関する優先度によりスクランブルモードを変更することによって、効果制御を実現できるとともに、パケット廃棄に対する影響を低減することができる。

【０１２４】また、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、優先度の高いパケットについてはスクランブルを行わず、優先度の低いパケットについてはスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、スクランブル鍵が存在する場合には優先度の低いパケットについてのみデスクランブルを行い、スクランブル鍵が存在しない場合には優先度の低いパケットを廃棄するデスクランブル装置とから構成されており、スクランブル装置においてパケット廃棄に関する優先度が低いパケットのみをスクランブルし、デスクランブル装置において、スクランブル鍵が存在する場合、すなわち視聴などの契約を行っている場合にはデスクランブルを行い、スクランブル鍵が存在しない場合、すなわち視聴などの契約を行っていない場合にはデスクランブル不可能な優先度の低いパケットは廃棄する。このようにすることによって、正規の受信者は優先度の高いパケットと優先度の低いパケットの両方を復号することができ、正規の受信者以外の受信者は優先度の高いパケットのみを復号することができる。従って、例えば原信号がディジタル映像信号のような信号の場合に、優先度の高いパケットに画像の低解像度の情報を、優先度の低いパケットに画像の低解像度の情報に追加する高解像度の情報をそれぞれ割り当てることによって、正規の受信者以外の受信者も低解像度の画像を視聴することが可能な効果制御を実現することができる。

【０１２５】また、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてデスクランブルを行うデスクランブル装置とから構成されており、パケット廃棄に関する優先度の高いパケットと低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルすることによって、ネットワーク中で優先度の低いパケットの廃棄が行われた場合にでも、優先度の高いパケットに影響を及ぼさないようにすることが可能となり、パケット廃棄への影響を低減することができる。

【０１２６】また、パケット廃棄に関する優先度をもつパケットにより構成される信号を入力とし、２つの連続するパケットを単位として処理し、２つのパケットのうち一方が優先度の高いパケットの場合には、両方とも優先度の高いパケットに書き換えて出力する信号処理装置と、信号処理装置からの信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてスクランブルを行うスクランブル装置と、スクランブル装置からのスクランブル信号を入力とし、優先度の高いパケットと優先度の低いパケットを別々の連鎖のある暗号方式の系列としてデスクランブルを行うデスクランブル装置とから構成されており、２つずつの連続したパケットを単位として処理を行うスクランブル伝送装置において、２つのパケットのうち一方が優先度の高いパケットの場合に両方とも優先度の高いパケットに書き換え、優先度の高いパケット単位と優先度の低いパケット単位とを別々の連鎖のある暗号方式の系列としてスクランブルし、優先度の低いパケットの廃棄の影響を低減することができる。すなわち、優先度の低いパケットの廃棄が行われた場合も、同じパケット単位内には優先度の高いパケットは含まれないため、同じパケット単位内の優先度の高いパケットには影響がなく、

優先度の高いパケット単位とは別の連鎖のある暗号方式の系列のため、次のパケット単位の優先度の高いパケットにも影響がない。

【図面の簡単な説明】

【図１】本発明の実施の形態１におけるスクランブル伝送装置の構成図である。

【図２】ＭＰＥＧ標準に準処した映像信号のピクチャーの構成図である。

【図３】ＭＰＥＧ標準に準処したトランスポートパケットの構成図である。

【図４】ＡＴＭセルの構成図である。

【図５】ＡＡＬ１によるＭＰＥＧ　ｏｖｅｒ　ＡＴＭの方式の説明図である。

【図６】ＡＡＬ５によるＭＰＥＧ　ｏｖｅｒ　ＡＴＭの方式の説明図である。

【図７】本発明の実施の形態２におけるスクランブル伝送装置の動作説明図である。

【図８】本発明の実施の形態３におけるスクランブル伝送装置の動作説明図である。

【図９】従来の技術における連鎖のあるブロック暗号方式（ＣＢＣモード）の説明図である。

【図１０】従来の技術におけるパケット廃棄による影響の問題の説明図である。

【符号の説明】

1a……符号化装置

1b……信号処理装置



＊1c……スクランブル装置

1d……優先度判定装置

1e……暗号化装置

1f……ＡＴＭアダプター

1g……ＡＴＭアダプター

1h……デスクランブル装置

1i……優先度判定装置

1j……暗号解読装置

1k……復号化装置

4a, 4b……トランスポートパケット

4c……ＣＰＣＳ－ＰＤＵトレーラー

4d, 4e, 4f, 4g, 4h, 4i, 4j, 4k……ＡＴＭセル

5a, 5e……Ｉピクチャー

5b, 5d……Ｂピクチャー

5c……Ｐピクチャー

6a……トランスポートパケット

7a……ＡＴＭセル

8a……トランスポートパケット

8b, 8c, 8d, 8e……ＡＴＭセル

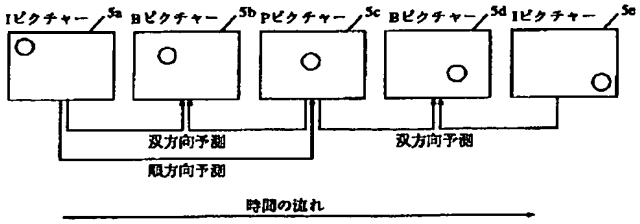
9a, 9c, 9e……優先パケット

9b, 9d……非優先パケット

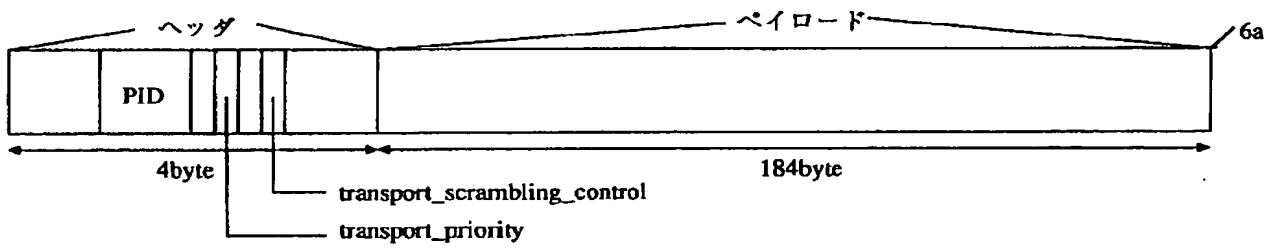
10a , 10e , 10f , 10i , 10m , 10n , 10q , 10r , 10u , 10v ……優先パケット

10b , 10c , 10d , 10g , 10h , 10j , 10k , 10l , 10o , 10p , 10s , 10t , 10w , 10x ……非優先パケット

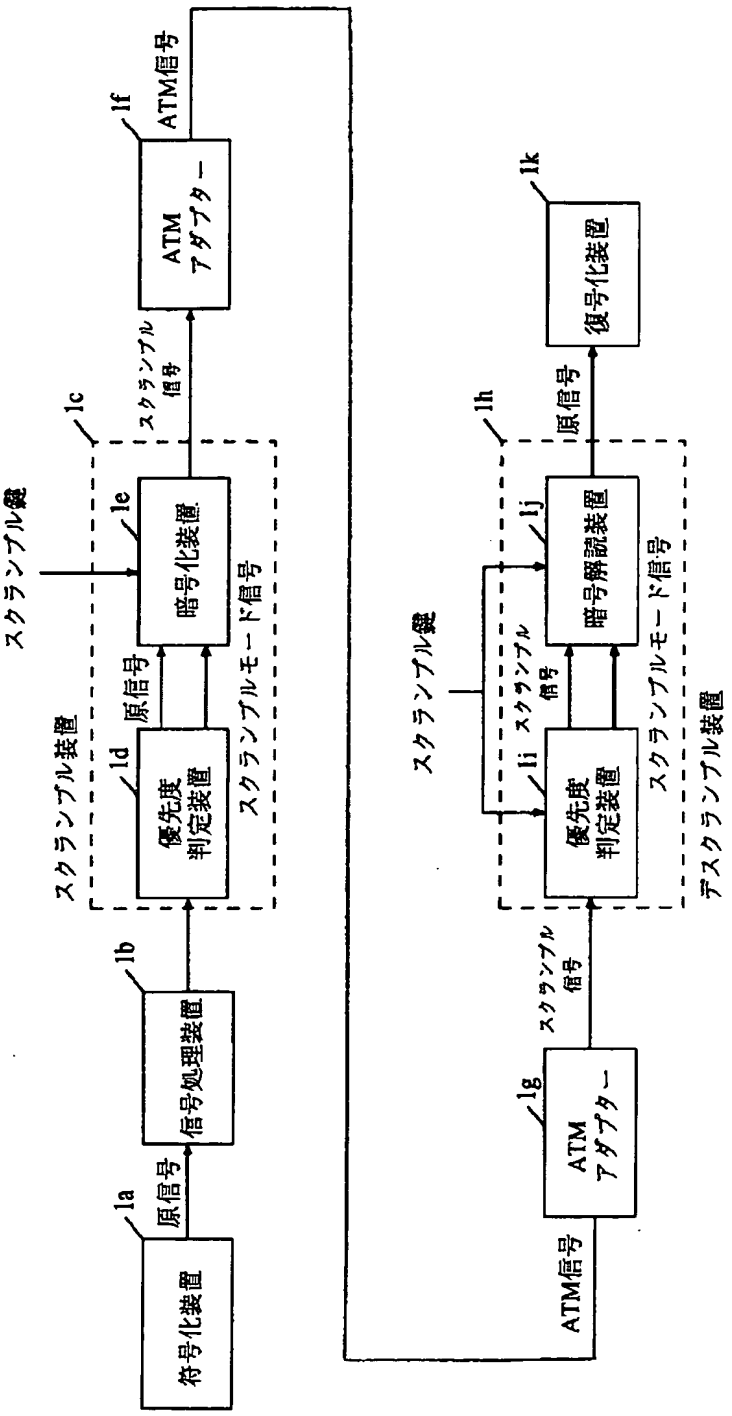
【図２】



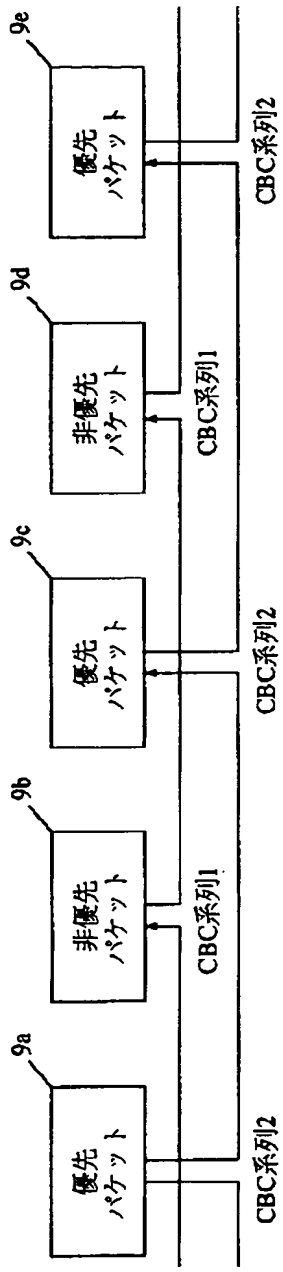

【図３】



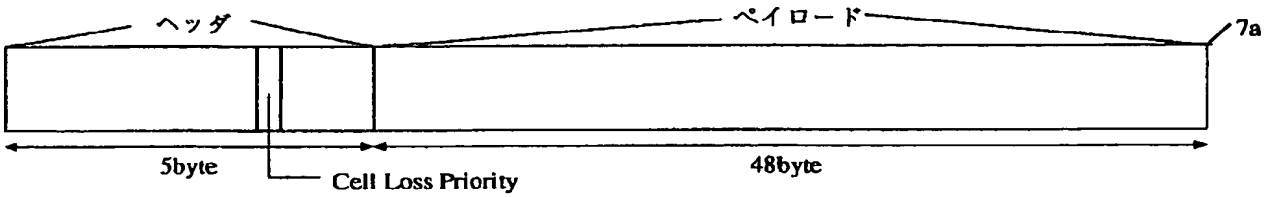
【図１】


スクランブル鍵
スクランブル装置
1a
符号化装置
原信号
1b
信号処理装置
1c
1d
優先度判定装置
原信号
1e
暗号化装置
スクランブル信号
スクランブルモード信号
1f
ATM信号
ATMアダプター
ATM信号
1g
ATMアダプター
スクランブル信号
スクランブル鍵
1h
1i
スクランブル信号
優先度判定装置
1j
暗号解読装置
原信号
1k
復号化装置
デスクランブル装置
スクランブルモード信号

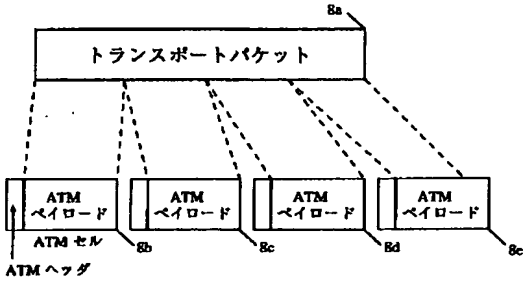
【図７】


9a
優先パケット
9b
非優先パケット
9c
優先パケット
9d
非優先パケット
9e
優先パケット
CBC系列1
CBC系列2
CBC系列1
CBC系列2

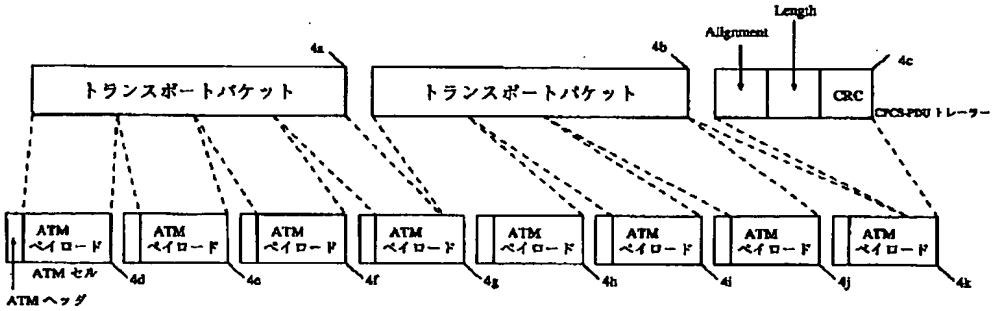
【図４】


ヘッダ
ペイロード
7a
5byte
Cell Loss Priority
48byte

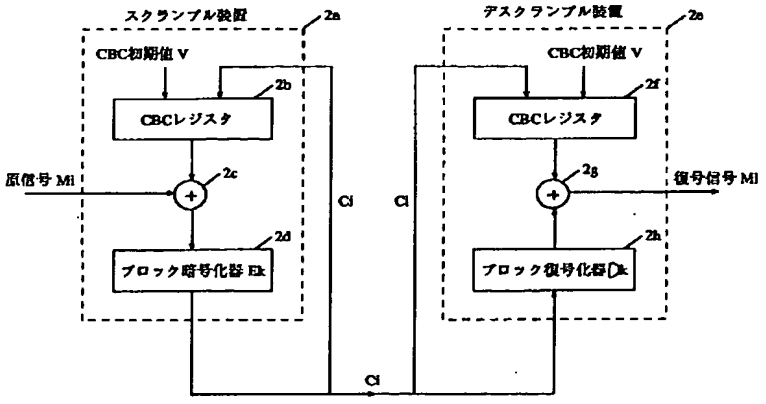
【図５】


8a
トランスポートパケット
ATM ペイロード
ATM セル
ATM ヘッダ
8b
8c
8d
8e

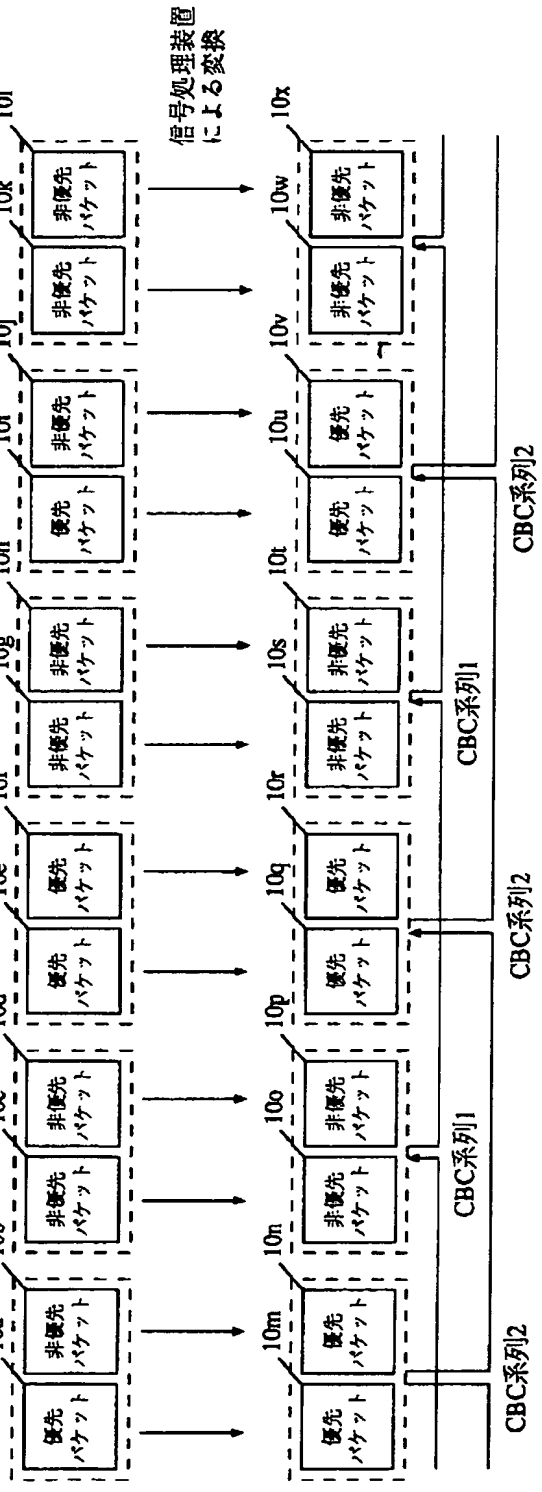
【図６】


4a
トランスポートパケット
4b
トランスポートパケット
Length
Alignment
CRC
4c
CPCS-PDU トレーラー
ATM ペイロード
ATM セル
ATM ヘッダ
4d
4e
4f
4g
4h
4i
4j
4k

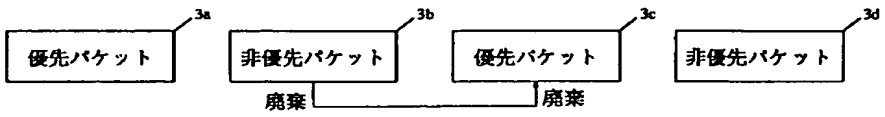
【図９】


スクランブル装置
2a
CBC初期値 V
2b
CBCレジスタ
2c
2d
ブロック暗号化器 Ek
CI
CI
CI
デスクランブル装置
2e
CBC初期値 V
2f
CBCレジスタ
2g
復号信号 MI
2h
ブロック復号化器 Dk

【図８】


信号処理装置による変換
10a
10b
10c
10d
10e
10f
10g
10h
10i
10j
10k
10l
10m
10n
10o
10p
10q
10r
10s
10t
10u
10v
10w
10x
優先パケット
非優先パケット
CBC系列1
CBC系列2
CBC系列1
CBC系列2

【図１０】




---

フロントページの続き

(72)発明者　茨木　晋
大阪府門真市大字門真1006番地　松下電器
産業株式会社内